STATEMENT

OF

GEORGE H. BOHLINGER, III
EXECUTIVE ASSOCIATE COMMISSIONER FOR MANAGEMENT
U.S. IMMIGRATION & NATURALIZATION SERVICE

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY

REGARDING
REVIEW OF COORDINATED INFORMATION SHARING
AND KNOWLEDGE MANAGEMENT ISSUES
FOR KEY FEDERAL AGENCIES
IN THE WAKE OF TERRORISM ATTACKS ON AMERICA

FRIDAY, JUNE 7, 2002

2154 RAYBURN HOUSE OFFICE BUILDING

10:00 A.M.

Good morning Mr. Chairman and members of the Committee.

I appreciate the opportunity to participate in your continuing review of "coordinated information sharing and knowledge management" between and among Federal agencies in the war against terrorism. I am particularly interested in addressing the Committee's desire to examine barriers that may hinder coordinated sharing and management, both within the Federal community, and between the Federal community and the private sector.

Since September 11, we at the Immigration and Naturalization Service (INS) have seen the unprecedented sharing of data and knowledge among federal agencies. Under the direction and leadership of the Attorney General, all components of the Department of Justice have stepped up efforts to coordinate information and improve data sharing in the common effort to prevent terrorism and disrupt its sources.

Congress signaled its support for these efforts by enacting the Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173) on May 14, 2002. As you know, this legislation requires the INS to fully integrate all of its databases and data systems that process or contain information on aliens. This integrated system will become part of the interoperable electronic data system, called Chimera. This system, when completed, will provide current and immediate access to information in law enforcement and intelligence databases relevant to determine whether to issue a visa and to determine the admissibility of an alien.

The INS is clearly one of the core agencies that requires enhanced information sharing capabilities. We need to tap into additional external sources of data to support our enforcement and intelligence functions, and we recognize that the data we collect can be crucial to the law enforcement and intelligence communities to combat the threat of terrorism.

Consequently, we are deeply involved in efforts to overcome the barriers to the appropriate and secure exchange of data and, just as important, the conversion of that data to useful information that supports clear operational objectives.

Mr. Chairman, before addressing the impediments to progress, let me begin by describing some important things we are already accomplishing in addressing these barriers.

As you know, the Office of Homeland Security, in conjunction with the Office of Management and Budget, is overseeing initiatives that promote information sharing between Federal agencies horizontally, and then from those agencies to State and local governments. We are working directly with State governments to improve the information available to support enforcement efforts. We are working internationally to develop better ways of sharing information that will support international enforcement and intelligence operations.

From my perspective, I cannot over-emphasize the commitment of the INS and other participants to work together in order to achieve a more supportive and comprehensive information environment.

Prior to September 11, the INS shared data in many ways with other agencies in support of law enforcement efforts. Since then we have redoubled our efforts to contribute data and information that have supported counter-terrorism intelligence, investigative, and enforcement operations.

One of the most important initiatives that we have worked on is the Foreign Terrorist Tracking Task Force (FTTTF), which the President directed the Department of Justice to establish on October 30, 2001. The mission of the FTTTF is to keep foreign terrorists and their supporters out of the United States by providing critical and timely information to border control and interior enforcement agencies and officials. To do so requires electronic access to large sets of data, including the most sensitive material from law

enforcement and intelligence sources. The INS works hand-in-hand with the FTTTF to discern patterns and probabilities of terrorist activities and to ensure that data is properly shared.

For many years, the INS has taken steps to enhance the exchange of information through greater cooperation among the law enforcement community. As early as 1985, the INS was sharing vital information with the U.S. Customs Service through the Interagency Border Inspection System (IBIS), the primary automated screening tool currently used by both of these agencies. Since that time, we have put in place a number of other initiatives to exchange information with other entities, which are in various stages of implementation.

For example, the INS and the Department of State recently expanded our ongoing datashare efforts. INS inspectors at ports-of-entry now have access to biometric data on all visa applicants, including digitized photographs, and are able to compare the photograph of the individual standing before them with the photograph of the individual who actually applied for the visa abroad.

Another example involves the sharing of fingerprint data. Prior to September 11, the INS had worked with the U.S. Marshals Service to incorporate fingerprint data of their wanted persons into the INS fingerprint identification system known as IDENT. After September 11, the INS worked with the Federal Bureau of Investigation (FBI) to incorporate fingerprint data from their Integrated Automated Fingerprint Information System (IAFIS) "wants and warrants" file into IDENT as well. IAFIS contains fingerprints for persons wanted by Federal, State, and local law enforcement agencies. This effort has been extremely successful and has already resulted in the identification and apprehension of over 1,600 individuals wanted for felony crimes.

One of the primary ways the INS assists State and local law enforcement is through the INS Law Enforcement Support Center (LESC). The primary mission of the LESC is to support other law enforcement agencies by helping them determine if a person they have contact with, or have in custody, is an illegal, criminal, or fugitive alien. The LESC provides a 24/7 link between Federal, State, and local officers and the databases maintained by the INS.

We also maintain a data sharing project with the Social Security Administration (SSA) through their participation in the INS Systematic Alien Verification for Entitlements (SAVE) program. Using the SAVE program, SSA has access to the Alien Status Verification Index, which provides alien status information. SSA uses this information to determine if a Social Security Number should be issued to a noncitizen applicant.

We also verify immigration status for State and local benefit granting agencies, some employers, and some State driver's license bureaus. For example, the INS has an ongoing data sharing initiative with the California Department of Motor Vehicles to enhance the integrity of their driver's license issuance process by providing information to verify that applicants are lawfully present at the time they apply for a license or State identification card.

We have intensified our efforts to share critical information with other law enforcement entities following the tragic events of September 11. We are coordinating with law enforcement officials at all levels -- Federal, State, and local – which are working together, coordinating information and sharing knowledge resources in the joint effort to avert and disrupt terrorist activity.

However, in all of these data sharing initiatives, we have to be sensitive to all established regulatory, statutory, and policy constraints in the routine and customary use of information by other agencies. When making information available to other entities, security, privacy considerations and appropriate user access are primary considerations. The INS has created a standing review body to ensure these issues are addressed with each data sharing request.

The Federal Government maintains a number of databases that provide real-time information to foreign diplomatic outposts, border points- of-entry, and interior domestic law enforcement. We work closely with these agencies to prevent terrorists from entering the United States, to detect and apprehend those already in the country, and to gather intelligence on terrorist plans and activities or conspiracies.

Examples of systems that share data include:

- The Department of State TIPOFF System--designed to detect known or suspected terrorists who are not U.S. citizens as they apply for visas overseas or as they attempt to pass through U.S., Canadian, and Australian border entry points.

- The FBI's National Crime Information Center--the nation's principal law enforcement automated information sharing tool. It provides on-the-street access to information to over 650,000 Federal, State, and local law enforcement officers.

- The Interagency Border Inspection System (IBIS)--the primary automated screening tool used by both the INS and U.S. Customs Service at ports-of-entry. The inclusion of terrorist data in this integrated database helps preclude the entry of known and suspected terrorists into the U.S., warn inspectors of a potential security threat, and alert intelligence and law enforcement agencies that a suspected terrorist is attempting to enter the U.S. at a specific location and time.

Mr. Chairman, having addressed what we have been doing to deal with the immediate challenges in response to guidance from Congress and the Administration, let me turn to the activities that address emergent issues on the horizon.

The management principle guiding the INS' approach to development of information systems is to build on a sound strategic foundation. The INS has established important mechanisms to address these principles internally. One of these mechanisms is our formal enterprise architecture and technical architectures, which are nearing completion. Additionally, an Information Technology Investment Management (ITIM) process has been in place for over three years. ITIM is the standardized process by which investment dollars are approved for information technology (IT) projects. This process ensures that IT investments are spent wisely and coordinated among INS components. In doing so, we are mindful of the relationships that we must support with our technical enhancements while integrating our business objectives and developing technical solutions.

ITIM and our formal enterprise and technical architectures will support the development of mission objectives. The development and prioritization of clear and integrated Federal law enforcement and intelligence missions is an undertaking that must be completed quickly. Only when these are clearly articulated can industry assist us meaningfully in applying the best technical solutions.

Some of the most compelling progress that I have seen in recent months has been formalization of the planning and management processes, as exemplified by the Attorney General's directive of April 11, 2002, to coordinate information relating to terrorism, that must occur if the wide array of Federal, State, local and private entities are to achieve the level of information sharing that we all desire. Structures are being developed that will bring discipline to the development and application of technology that will ensure we first define what our operational objectives should be, identify the data and the data sources needed to support those objectives, and then apply the appropriate technology solutions to deliver that information.

As I stated previously, I am particularly interested in examining and understanding what barriers may exist that inhibit, or otherwise thwart, full partnership between the public and private sectors in coming

together in the war against terrorism. Like many of my colleagues, I have met with a myriad of representatives from the private sector who have proffered technologically-based products and solutions to any number of counter-terrorism driven prevention, detection, and mitigation scenarios. Their sincerity and commitment are of the highest order. Unfortunately, in many instances, they perceive the Federal Government as an unresponsive bureaucracy.

Some have suggested that the Federal procurement process may be to blame. However, I believe it would be a mistake to look at the procurement process as the culprit. If clear requirements can be formulated, many procurement alternatives are available that can fulfill our needs, while ensuring broad participation by industry.

One example of identifying our requirements is in the implementation of the Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173). The INS is in the process of identifying information needs from Federal law enforcement and the intelligence community to improve national security. We continue to value private sector input through the Request for Information process prior to initiation of a formal procurement process, while preserving a fully fair and open procurement process.

There are a number of information technology professional associations that provide venues for exchange of issues, discussions of requirements and development of ideas. The INS is fully engaged in these opportunities. We have been steadfast in articulating our position to industry, and our willingness to engage in active and meaningful partnerships, not only during procurements, but also post award.

In summary, we in the Federal Government must establish and employ standards for information sharing between and among ourselves and further, fully define the mission requirements or needs. Then we can take advantage of the wealth of existing technology solutions that are already out there, but which may be imbedded within individual agencies and corporations. This will enable us to knit solutions together in a meaningful way to better balance our openness to new ideas with focus on applications which directly address our needs.

Thank you Mr. Chairman for this opportunity to share my views with you and the Committee.

#